EXHIBIT 6

Date of Hearing: June 21, 2005

ASSEMBLY COMMITTEE ON BUSINESS AND PROFESSIONS
Gloria Negrete McLeod, Chair
SB 355 (Murray) - As Amended: June 15, 2005

SENATE VOTE : 37-2

SUBJECT : Internet regulation: Anti-Phishing Act of 2005.

SUMMARY : Establishes the Anti-Phishing Act of 2005, which makes it unlawful for any person, through the Internet or other electronic means, to solicit, request, or take any action to induce another person to provide identifying information, by representing itself to be an online business without the approval or authority of the online business. Specifically, this bill :

1)Provides that it is unlawful for a person to use a Web page, email, or the Internet to misrepresent that he or she is an online business and solicit or induce another person to provide his or her personal information without the authority or approval of the online business.

2)Provides that the following persons may bring an action against a person who violates, or is in violation of, this code section:

a) A person who: i) is engaged in the business of providing Internet access service to the public, owns a Web page, or owns a trademark; and, ii) is adversely affected by a violation of the code section; and,

b) An individual who is adversely affected by a violation of the provisions of this code section, but such an individual may only bring an action against a person who has directly violated this code section.

3)Provides that an action brought under this code section by a person who is engaged in the business of providing Internet access service to the public, owns a Web page, or owns a trademark, may seek to recover the greater of actual damages or $500,000.

4)Provides that an action brought by an individual who is

adversely affected by a violation of the provisions of this code section may seek to enjoin further violations of those provisions and recover the greater of three times the amount of actual damages, or $5,000 per violation.

5)Provides that the Attorney General or a district attorney may bring an action against a person who violates, or is in violation of, the provisions of this code section to enjoin further violations of those provisions and to recover a civil penalty of up to $2,500 per violation. A court may, in addition, do either or both of the following:

a) Increase the recoverable damages to an amount up to three times the damages otherwise recoverable in cases that the defendant has engaged in a pattern and practice of violating the provisions of this code section; and,

b) Award costs of suit and reasonable attorney's fees to a prevailing plaintiff.

6)Specifies that the remedies provided in this code section do not preclude the seeking of remedies, including criminal remedies, under any other applicable provision of law.

7)Provides that multiple violations of the provisions of this section resulting from any single action or conduct shall constitute one violation of this code section when the action is brought by a person who is engaged in the business of providing Internet access service to the public, owns a Web page, or owns a trademark.

EXISTING LAW :

1)Does not regulate "phishing" actions, but makes fraud actionable where the following has been established: (a) a misrepresentation; (b) knowledge of falsity; (c) intent to defraud, i.e., to induce reliance; (d) justifiable reliance; or, (e) resulting damage.

2)Provides that the Attorney General or a district attorney can

seek an injunction and civil penalties of up to $2,500 per instance for any unlawful business act or practice. An individual may seek an injunction for an unlawful business act or practice if he or she suffered an injury in fact and lost money or property as a result.

FISCAL EFFECT : Unknown

COMMENTS :

Background . "Phishing" is a widespread technique for obtaining personal information, and is used to facilitate identity theft and other crimes. Phishers use fraudulent emails or Web sites to trick consumers into providing personal information, such as bank account numbers and social security numbers, to what is believed to be a legitimate company.

The author's office explains, "Customers often receive a legitimate looking email that appears to be from their bank or [a] retailer with whom they do business. The consumer is often told via e-mail that a review of their account found "unusual activity" and directs them to a phony website where they are compelled to provide personal information such as their name, account number and other relevant data. Criminals have become very good at mimicking legitimate emails and setting identical Web sites."

Support . The author's office states, "According to the FBI and the Internet Crime Complaint Center, 78% of all criminal 'phishers' are located in the United States. Of these, 15% of all phishing scams originate in California, the most in the nation. In 2004 alone, there were over 100,000 reports of this fraud with over 76,000 consumers losing money. In reported cases alone, consumers lost over $193 million in 2003 and 2004. The California Alliance for Consumer Protection notes it has received numerous complaints in recent weeks from consumers who filled out forms on false "eBay web pages' with their personal information, thinking that those pages were authentic."

The Computing Technology Industry Association (CompTIA) states, "Billions of dollars of Californian commerce, jobs and productivity gains are tied to the spread of Internet commerce and communications. Confidence in the integrity of personal information transmitted via the Internet remains an integral part of the medium's development. However, recent independent studies, polls and national news reports reveal that phishing is greatly undermining that confidence, phishing tops the concerns of many inside and outside of the IT industry as potentially hobbling the Internet's exciting growth."

CompTIA notes that this bill "puts real 'teeth'" into its prohibitions by making each separate violation punishable by $500,000 in damages, and tripling damages where a pattern of phishing has been established.

Microsoft states it is important to enact legislation to combat the threat of phishing, in addition to using other tools such as technology innovation, targeted enforcement, and user education. Microsoft contends that the "[s]trong laws and adequate enforcement" provided by SB 355 will be critical to addressing the phishing problem.

REGISTERED SUPPORT / OPPOSITION :

Support

AeA
California Alliance for Consumer Protection
CompTIA
Microsoft

Opposition

None on file.

Analysis Prepared by : Tracy Rhine / B. & P. / (916) 319-3301